druva

GDPR Shared Responsibility model

Article	Article Summary	Customer's Responsibility	Druva (inSync)	Druva (Phoenix)
General Provisions				
1	Subject-matter and objectives –– This Regulation contains rules on processing personal data and the free movement of personal data to protect the fundamental rights and freedoms of natural persons and their right to protection of personal data	As a global organization with customers all over the world, including in the European Union, Druva is subject to the GDPR when it comes to processing data of the European Union data subjects. Since Druva has no access to unencrypted data due to the envelope encryption method, Druva cannot distinguish what kind of data is being processed through the use of Druva's product offerings. It is Customer's responsibility to notify Druva of its intent to use Druva's products to process personal data of the European Union data subjects.		
2	Material Scope –– This Regulation applies to the processing of personal data which form part of a filing system.			
3	Territorial Scope –– This Regulation applies to controllers and processors in the Union and controllers or processors not in the Union if they process personal data of data subjects who live in the Union			
4	Definitions: https://gdpr-info.eu/art-4-gdpr/			
General Principles				
5	Principles relating to processing of personal data –– Personal data shall be processed lawfully, fairly, and in a transparent manner; collected for specified, explicit, and legitimate purposes; be adequate, relevant, and limited to what is necessary; etc.	Customer is responsible for collecting personal data in a lawful, fair, and transparent manner for a specified, explicit, and legitimate purposes consistent with data minimization principle. Druva's products are designed to enable customers to manage the data processed through the admin settings. Due to Druva's envelope encryption model, Druva does not have access to any unencrypted customer data, which may include personal data. As such, Druva will never process customer data in any way that is inconsistent with the purpose of processing - data backup, protection, and management.		
6	Lawfulness of processing –– There are six reasons that make processing lawful if at least one is true (e.g. data subject has given consent, processing is necessary for the performance of a contract, etc).	Druva allows the customer administrators to control and upload only the content they want to backup and manage through the product settings. Customers should identify the type of data they backup and manage through Druva's product offering and confirm that the processing falls within one of the six reasons that make the processing lawful.	When a customer uses Druva's product offerings, both Druva and customer enter into an agreement pursuant to which Druva processes customer data, which may include personal data.	
7	Conditions for Consent –– When processing is based on consent, whoever controls the personal data must prove consent to the processing, and the data subject can withdraw consent at any time.	It is customer's responsibility to ensure that the data subjects have freely consented to processing as well as managing individuals' right to revoke such consent.	While Druva has no access to customer's unencrypted data, due to Druva's envelope encryption method, Druva InSync allows customers to determine which data is processed through Druva's cloud services. inSync customer can choose how much control they leave to end users as to which data is backed up. inSync also allows customers to leave it completely to end users to define which data to backup and which data not to. In addition, Customers may also configure inSync so that end users choose whether inSync admins have access to their data. Should Customer choose to force a backup policy on its end users, customer needs to obtain end user's consent. For Cloud Apps data it is customer's responsibility to obtain end user's consent for processing.	While Druva has no access to customer's unencrypted data, due to Druva's envelope encryption method, Druva Phoenix allows customers to determine which data is processed through Druva's cloud services.
8	Conditions applicable to child's consent in relation to information societal services –– Information society services can process personal data of a child if the child is over 16. If the child is under 16, the legal guardian must consent.	Customers must ensure that personal data of children is processed appropriately and that end users have provided appropriate notices and obtained where applicable parental consent requirements.	Druva InSync enables customers to control and upload only the data they want to process through Druva's cloud services. Druva does not differentiate or separate the types of personal data processed by customers, so customers must ensure that personal data of children is processed appropriately and that end users have provided appropriate notices and obtained where applicable parental consent requirements.	Druva Phoenix enables customers to control and upload only the data they want to process through Druva's cloud services. Druva does not differentiate or separate the types of personal data processed by customers, so customers must ensure that personal data of children is processed appropriately and that data subjects have provided appropriate notices and obtained where applicable parental consent requirements.

Article	Article Summary	Customer's Responsibility	Druva (inSync)	Druva (Phoenix)
9	Processing special categories of personal data –– Processing personal data revealing race, political opinions, religion, philosophy, trade union membership, genetic data, health, sex life, and sexual orientation is prohibited unless the subject gives explicit consent, it's necessary to carry out the obligations of the controller, it's necessary to protect the vital interests of the data subject, etc.	It is customer's responsibility to ensure that the data subjects have freely consented to processing sensitive data as well as managing individuals' right to revoke such consent.	While Druva has no access to customer's unencrypted data, due to Druva's envelope encryption method, Druva InSync allows customers to determine which data is processed through Druva's cloud services. inSync customer can choose how much control they leave to end users as to which data is backed up. inSync also allows customers to leave it completely to end users to define which data to backup and which data not to. In addition, Customers may also configure inSync so that end users choose whether inSync admins have access to their data. Should Customer choose to force a backup policy on its end users, customer needs to obtain end user's explicit consent. In addition, inSync Elite + customers can use PII templates using our proactive compliance module - to identify a limited set of data elements and choose to eliminate them from processing (delete/quarantine). For Cloud Apps data it is customer's responsibility to obtain end user's consent for processing.	While Druva has no access to customer's unencrypted data, due to Druva's envelope encryption method, Druva Phoenix allows customers to determine which data is processed through Druva's cloud services. As such, it is customer's responsibility to ensure compliance for processing of sensitive data.
10	Processing personal data related to criminal convictions and offenses –– Processing personal data related to criminal convictions can only be carried out by an official authority or when Union or Member State law authorizes the processing.	It is customer's responsibility to ensure that they have the official authority to process criminal convictions data or compliance with Union or Member State laws.	While Druva has no access to customer's unencrypted data, due to Druva's envelope encryption method, Druva InSync allows customers to determine which data is processed through Druva's cloud services. Should Customer choose to force a backup policy on its end users, customer needs to ensure compliance with applicable Union or Member State laws with regards to processing of criminal convictions data. For Cloud Apps data it is customer's responsibility to ensure compliance for processing of criminal convictions data.	While Druva has no access to customer's unencrypted data, due to Druva's envelope encryption method, Druva Phoenix allows customers to determine which data is processed through Druva's cloud services. As such, it is customer's responsibility to ensure compliance for processing of criminal convictions data.
11	Processing which does not require identification –– The controller does not need to get or process additional information to identify the data subject if the purpose for which the controller processes data does not require the identification of a data subject.	It is customer's responsibility to ensure that the data collected or processed through Druva's products is consistent with the purpose of processing.		
	Rights of Data Subject			
12	Transparent information, communications, and modalities for the exercise of the rights of the data subject –– When necessary, the controller must provide information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, and the controller needs to provide information on action taken on request by and to the data subject within one month.	It is customer's responsibility to ensure compliance with this article. If a data subject sends a request to exercise rights with regards to such data subject's personal data, Druva shall communicate such request to customer as soon as possible to allow compliance with this article.		
13	Information to be provided where personal data are collected from the data subject –– When personal data is collected from the data subject, certain information needs to be provided to the data subject.	It is customer's responsibility to provide proper privacy notices at the point of data collection from data subjects. Druva's privacy policy can be found at https://www.druva.com/privacy-policy/		
14	Information to provide to the data subject when personal data has not been obtained from data subject –– When personal data is not obtained from the data subject, the controller has to provide the data subject with certain information.			
15	Right of access by the data subject –– The data subject has a right to know whether their personal data is being processed, what data is being processed, etc.	It is customer's responsibility to respond to data subject's request to access data subject's personal data.	Druva does not have access to the customer data processed by using Druva's cloud services. As such, any individual data requests to access data must be managed by the InSync Admin.	"Druva does not have access to the customer data stored by using Druva's cloud services. As such, any individual data requests to access data must be managed by the Phoenix Admin.
16	Right to rectification –– The data subject can require the controller to rectify any inaccurate information immediately.	It is customer's responsibility to respond to data subject's request to rectify any inaccurate information.	Druva does not have access to the customer data processed by using Druva's cloud services. As such, any individual data requests to correct data must be managed by the InSync Admin.	Druva does not have access to the customer data stored by using Druva's cloud services. As such, any individual data requests to correct data must be managed by the Phoenix Admin.

Article	Article Summary	Customer's Responsibility	Druva (inSync)	Druva (Phoenix)
17	Right to be forgotten –– In some cases, the data subject has the right to make the controller erase all personal data, with some exceptions.	It is customer's responsibility to ensure compliance with this article. Druva's products can be used to help comply with this requirement.	Druva does not have access to the customer data stored by using Druva's cloud services. As such, any individual data requests must be managed by the inSync admin. The following options should help the inSync admin to a data subject's withdrawal of consent. Options for customers: A. Data subject can create a folder and move all of the personal data into that folder. Admin then deletes the folder. B. inSync admin can go Print_Area Availability-> Restore, search for the user, and then manage their snapshots. This would allow the inSync admin to delete all of the data subject's data. Proactive compliance + Elite customers (excluding Cloud Apps): If the admin knows the particular file name, the admin can search within Governance -> Enterprise Search, filter by metadata if needed and then the admin will have the option of deleting the file from source and/or snapshots.	Druva does not have access to the customer data stored by using Druva's cloud services. As such, any individual data requests must be managed by the Phoenix Admin.
18	Right to restriction of processing –– In some cases, the data subject can restrict the controller from processing.	It is customer's responsibility as a data controller to ensure compliance with these articles.		
19	Notification obligation regarding rectification or erasure of personal data or restriction of processing –– The controller has to notify recipients of personal data if that data is rectified or erased.			
20	Right to data portability –– The data subject can request to receive their personal data and give it to another controller or have the current controller give it directly to another controller.	It is customer's responsibility to ensure compliance with this article. Druva's products can be used to help comply with this requirement.	Druva does not have access to the customer data stored by using Druva's cloud services. As such, any individual data requests must be managed by the inSync admin. The following process should help the inSync Admin to an individual's request to transmit individual's data to another service provider. InSync admin can go into Availability-> Restore, search for the user, and then manage their snapshots. This would allow the admin to upload the data onto individual's electronic portable device.	Druva does not have access to the customer data stored by using Druva's cloud services. As such, any individual data requests must be managed by the Phoenix admin.
21	Right to Object –– Data subjects have the right to object to data processing on the grounds of his or her personal situation.	It is customer's responsibility to ensure compliance with this article.	If Druva receives data subject's objection to processing, Druva will communicate such request to customer as soon as possible to allow compliance with this article.	
22	Automated individual decision-making, including profiling –– Data subjects have the right not to be subjected to automated individual decision-making, including profiling.	It is customer's responsibility to ensure compliance with this article.	Druva does not engage in automated individual decision-making.	
23	Restrictions –– Union or Member State law can restrict the rights in Articles 12 through 22 through a legislative measure.	It is customer's responsibility to stay abreast of the applicable Member State laws as they apply to the content of customer data and the responsibilities of the controller.	Druva relies on customer's instructions with regards to processing customer data in accordance with specific Member State laws.	
	Controller and Processor			
24	Responsibility of the Controller –– The controller has to ensure that processing is in accordance with this Regulation.	As between Druva and customer, customer is the data controller and Druva is the data processor when it comes to customer data processed through Druva's products and services.		
25	Data protection by design and by default –– Controllers must implement data protection principles in an effective manner and integrate necessary safeguards to protect rights of data subjects.	It is customer's responsibility as a data controller to ensure security of personal data.	Druva maintains appropriate technical and organizational safeguards to protect the security, confidentiality and integrity of Customer Data, including any personal data contained therein. Such measures are designed to protect Customer Data from loss, alteration, unauthorized access, acquisition, use, disclosure, or accidental or unlawful destruction. Such measures include, but are not limited to logical data segregation, data encryption in flight and at rest, network security, security logging and monitoring, envelope encryption model, and regular third party penetration testing. For more information on Druva's security protocols, please email security@druva.com or review Druva's security White Papers https://www.druva.com/resources/white-papers/.	
26	Joint Controllers –– When there are two or more controllers they have to determine their respective responsibilities for compliance.	N/A		

Article	Article Summary	Customer's Responsibility	Druva (inSync)	Druva (Phoenix)
27	Representatives of controllers or processors not established in the Union –– When the controller and processor are not in the Union, in most cases they have to establish a representative in the Union.	It is customer's responsibility to ensure compliance with this article.	Druva has established presence in the European Union and the United Kingdom.	
28	Processor –– When processing is carried out on behalf of a controller, the controller can only use a processor that provides sufficient guarantees to implement appropriate technical and organizational measures that will meet GDPR requirements.	Druva is committed to meeting the GDPR requirements. To request Druva's Data Processing Agreement, please email privacy@druva.com		
29	Processing under the authority of the controller or processor –– Processors can only process data when instructed by the controller.	Druva only processes personal data in accordance with customer's instructions and to the extent necessary for providing the cloud services as described in the applicable customer agreement. The agreement and any additional data processing instructions provided by customer constitute "instructions," so long as any additional or alternate instructions are consistent with the purpose and scope of the agreement and are provided and/or confirmed in writing by the Customer.		
30	Records of Processing Activities –– Each controller or their representatives needs to maintain a record of processing activities and all categories of processing activities.	It is customer's responsibility to ensure compliance with this article.	Through the inSync admin functionalities, Druva inSync enables users to control what data is stored and processed through cloud services. Customers are responsible for maintaining an inventory of the personal data processed through Druva's cloud services . Druva maintains immutable audit logs, accessible only by the customer, providing a trail of all processing actions.	Through the Phoenix admin functionalities, Druva Phoenix enables users to control what data is stored and processed through cloud services. Customers are responsible for maintaining an inventory of the personal data processed through Druva's cloud services. Druva maintains immutable audit logs, accessible only by the customer, providing a trail of all processing actions.
31	Cooperation with the supervisory authority –– The controller and processor have to cooperate with supervisory authorities.	It is Druva's and customer's shared responsibility to cooperate with supervisory authorities. In the case of an audit, inquiry or investigation by a government body, data protection authority or law enforcement agency regarding the processing of Personal Data, Druva shall promptly notify customer unless prohibited by applicable law. Customer shall cooperate and provide all necessary information and records to Druva in the event Druva is required to produce any records of Personal Data processed by Druva to a data protection authority. Customer shall reimburse Druva for any reasonable additional costs incurred in connection with the fulfilment of Druva's obligations .		
32	Security of processing –– The controller and processor must ensure a level of security appropriate to the risk.	It is customer's responsibility to maintain appropriate internal security protocols to safeguard customer's personal data. Druva's products and services help customer to protect customer data processed through Druva's product offering.	Druva maintains appropriate technical and organizational safeguards to protect the security, confidentiality and integrity of Customer Data, including any personal data contained therein. Such measures are designed to protect Customer Data from loss, alteration, unauthorized access, acquisition, use, disclosure, or accidental or unlawful destruction. Such measures include, but are not limited to logical data segregation, data encryption in flight and at rest, network security, security logging and monitoring, envelope encryption model, and regular third party penetration testing. For more information on Druva's security protocols, please email security@druva.com or review Druva's security White Papers https://www.druva.com/resources/white-papers/.	
33	Notification of a personal data breach to the supervisory authority –– In the case of a breach, the controller has to notify the supervisory authority within 72 hours, unless the breach is unlikely to result in risk to people. And the processor needs to notify the controller immediately.	It is customer's responsibility to inform the applicable supervisory authority of the breach reported to customer by Druva.	Druva shall report to customer any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to customer data that it becomes aware of without undue delay (not to exceed 48 hours).	
34	Communication of a personal data breach to the data subject –– When a breach is likely to cause risk to people, the controller has to notify data subjects immediately.	It is customer's responsibility to ensure compliance with this article. Druva will reasonably cooperate with customer's requests for information and reporting on any security incident that is likely to result in risk to people		
35	Data protection impact assessment –– When a type of processing, especially with new technologies, is likely to result in a high risk for people, an assessment of the impact of the processing needs to be done.	Effective from May 25, 2018, upon customer's request, Druva will provide customer with reasonable cooperation and assistance needed to fulfil customer's obligation under the GDPR to carry out a data protection impact assessment related to customer's use of the cloud services to the extent customer does not have access to such information without Druva's assistance.		
36	Prior consultation –– The controller needs to consult the supervisory authority when an impact assessment suggests there will be high risk if further action is not taken. The supervisory authority must provide advice within eight weeks of receiving the request for consultation.	It is customer's responsibility to ensure compliance with this article.		
37	Designation of the data protection officer –– The controller and processor must designate a data protection officer (DPO) if processing is carried out by a public authority, processing operations require the systematic monitoring of data subjects, or core activities of the controller or processor consist of processing personal data relating to criminal convictions or on a large scale of special categories of data pursuant to Article 9.	Customers must appoint a data protection officer to ensure their compliance with the GDPR. Druva has appointed a data protection officer who can be contacted at privacy@druva.com		
38	Position of the data protection officer –– The DPO must be involved in all issues which relate to the protection of personal data. The controller and processor must provide all necessary support for the DPO to do their tasks and not provide instruction regarding those tasks.			

Article	Article Summary	Customer's Responsibility	Druva (inSync)	Druva (Phoenix)
39	Tasks of the data protection officer –– The DPO must inform and advise the controller and processor and their employees of their obligations, monitor compliance, provide advice, cooperate with the supervisory authority, and act as the contact point for the supervisory authority.	These articles establish the role of supervisory authorities in drawing codes of conduct as well as the role of Member States in issuance of GDPR compliance certifications. They are provided for infromative purposes only.		
40	Codes of conduct –– Member States, the supervisory authorities, the Board, and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR.			
41	Monitoring of approved codes of conduct –– A body with adequate expertise in the subject-matter and is accredited to do so by the supervisory authority can monitor compliance with a code of conduct.			
42	Certification –– Member States, the supervisory authorities, the Board, and the Commission shall encourage the establishment of data protection certification mechanisms to demonstrate compliance.			
43	Certification bodies –– Certification bodies accredited by Member States can issue and renew certifications.			
Transfers of Personal Data				
44	General principle for transfers –– Controllers and processors can only transfer personal data if they comply with the conditions in this chapter.	It is customer's responsibility to ensure data transfer in compliance with this chapter.	Sub-Processors. Druva requires sub-processors to abide by the Standard Contractual Clauses for data processors established in third countries or another lawful mechanism for the transfer of Personal Data as approved by the European Commission. Druva. Druva complies with the EU-U.S. Privacy Shield Framework set forth by the United States Department of Commerce or the Standard Contractual Clauses (if executed between the parties). In addition, customer may choose to store customer data within the European Union by choosing data centers located within the EEA territory.	
45	Transfers on the basis of an adequacy decision –– A transfer of personal data to a third country or international organization can occur if the Commission has decided the country or organization can ensure an adequate level of protection.			
46	Transfers subject to appropriate safeguards –– If the Commission has decided it can't ensure an adequate level of protection, a controller or processor can transfer personal data to a third country or organization if it has provided appropriate safeguards.			
47	Binding Corporate rules –– The supervisory authority will approve binding corporate rules in accordance with the consistency mechanism in Article 63.			
48	Transfers or disclosures not authorized by Union law –– Any decision by a court or administrative authority in a third country to transfer or disclose personal data is only enforceable if the decision is based on an international agreement.			
49	Derogations for specific situations –– If there is no adequacy decision (Article 45) or appropriate safegaurds, a transfer of personal data to a third country or organization can only happen if one of seven certain conditions are met.			
50	International cooperation for the protection of personal data –– The Commission and supervisory authority have to do their best to further cooperation with third countries and international organizations.			
Independent Supervisory Authority				
51	Supervisory authority –– Each Member state has to supply at least one independent public authority to enforce this regulation.	These provisions relate to the function of the supervisory authority and are provided for informative purposes.		
52	Independence –– Each supervisory authority has to act with complete independence, and its members have to remain free from external influence.			
53	General conditions for the members of the supervisory authority –– Member states need to appoint members of the supervisory authority in a transparent way, and each member must be qualified.			

Article	Article Summary	Customer's Responsibility	Druva (inSync)	Druva (Phoenix)
54	Rules on the establishment of the supervisory authority –– Each Member State needs to provide, in law, the establishment of each supervisory authority, qualifications for members, rules for appointment, etc.	These provisions relate to the function of the supervisory authority and are provided for informative purposes.		
55	Competence –– Each supervisory authority must be competent to perform the tasks in this Regulation.			
56	Competence of the lead supervisory authority –– The supervisory authority of a controller or processor that is doing cross-border processing will be the lead supervisory authority.			
57	Tasks –– In its territory, each supervisory authority will monitor and enforce this Regulation, promote public awareness, advise the national government, provide information to data subjects, etc.			
58	Powers –– Each supervisory will have investigative, corrective, authorization, and advisory powers.			
59	Activity Reports –– Each supervisory authority must write an annual report on its activities.			
	Cooperation and Consistency			
60	Cooperation between the lead supervisory authority and the other supervisory authorities concerned –– The lead supervisory authority will cooperate with other supervisory authorities to attain information, mutual assistance, communicate relevant information, etc.	These provisions describe the relationship between the supervosory authorities, the Commission, and the European Data Protection Board. They are provided for informative purposes only.		
61	Mutual assistance –– Supervisory authorities must provide each other with relevant information and mutual assistance in order to implement and apply this regulation.			
62	Joint operations of supervisory authorities –– Where appropriate, supervisory authorities will conduct joint operations.			
63	Consistency mechanism –– For consistent application of this Regulation, supervisory authorities will cooperate with each other and the Commission through the consistency mechanism in this section.			
64	Opinion of the Board –– If a supervisory authority adopts any new measures, the Board will issue an opinion on it.			
65	Dispute resolution by the Board –– The Board has the power to resolve disputes between supervisory authorities.			
66	Urgency Procedure –– If there is an urgent need to act to protect data subjects, a supervisory authority may adopt provisional measures for legal effects that do not exceed three months.			
67	Exchange of information –– The Commission may adopt implementing acts in order to specify the arrangements for the exchange of information between supervisory authorities.			
68	European Data Protection Board –– The Board is composed of the head of one supervisory authority from each Member state.			
69	Independence –– The Board must act independently when performing its tasks or exercising its powers.			
70	Tasks of the Board –– The Board needs to monitor and ensure correct application of this Regulation, advise the Commission, issue guidelines, recommendations, and best practices, etc.			
71	Reports –– The Board will write an annual public report on the protection of natural persons with regard to processing.			
72	Procedure –– The Board will consider decisions by a majority vote and adopt decisions by a two-thirds majority.			
73	Chair –– The Board elects a chair and two deputy chairs by a majority vote. Terms are five years and are renewable once.			

Article	Article Summary	Customer's Responsibility	Druva (inSync)	Druva (Phoenix)
74	Tasks of the chair –– The Chair is responsible for setting up Board meetings, notifying supervisory authorities of Board decisions, and makes sure Board tasks are performed on time.	These provisions describe the relationship between the supervosory authorities, the Commission, and the European Data Protection Board. They are provided for informative purposes only.		
75	Secretariat –– The European Data Protection Supervisor will appoint a secretariat that exclusively performs tasks under the instruction of the Chair of the Board, mainly to provide analytical, administrative, and logistical support to the Board.			
76	Confidentiality –– Board discussions are confidential.			
	Remedies Liability and Penalties			
77	Right to lodge a complaint with a supervisory authority –– Every data subject has the right to lodge a complaint with a supervisory authority.	These provisions outline the process for penalties for failure to comply with the GDPR as well as individual's right to seek remedies against data controllers and processors. These provisions are provided for informative purposes only.		
78	Right to an effective judicial remedy against a supervisory authority –– Each natural or legal person has the right to a judicial remedy against a decision of a supervisory authority.			
79	Right to an effective judicial remedy against a controller or processor –– Each data subject has the right to a judicial remedy if the person considers his or her rights have been infringed on as a result of non-compliance processing.			
80	Representation of data subjects –– Data subjects have the right to have an organization lodge a complaint on his or her behalf.			
81	Suspension of proceedings –– Any court in a Member State that realizes proceedings for the same subject that is already occurring in another Member State can suspend its proceedings.			
82	Right to compensation and liability –– Any person who has suffered damage from infringement of this Regulation has the right to receive compensation from the controller or processor or both.			
83	General conditions for imposing administrative fines –– Each supervisory authority shall ensure that fines are effective, proportionate, and dissuasive. For infringements of Articles 8, 11, 25 to 39, 41, 42, and 43 fines can be up to €10,000,000 or two percent global annual turnover. For infringements of Articles 5, 6, 7, 9, 12, 22, 44 to 49, and 58 fines can be up to €20,000,000 or four percent of global annual turnover.			
84	Penalties –– Member States can make additional penalties for infringements.			
	Specific Processing Situations			
85	Processing and freedom of expression and information –– Member States have to reconcile the protection of personal data and the right to freedom of expression and information (for journalistic, artistic, academic, and literary purposes).	These provisions are addressing Member States' right to implement more restrictive regulations with regards to processing of certain types of data. They also address special public purposes in the public interest. These provisions are provided for informative purposes only.		
86	Processing and public access to official documents –– Personal data in official documents for tasks carried out in the public interest may be disclosed for public access in accordance with Union or Member State.			
87	Processing of the national identification number –– Member States can determine the conditions for processing national identification numbers or any other identifier.			
88	Processing in the context of employment –– Member States can provide more specific rules for processing employees' personal data.			
89	Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes –– Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is subject to appropriate safeguards (data minimization and pseudonymization).			

Article	Article Summary	Customer's Responsibility	Druva (inSync)	Druva (Phoenix)
90	Obligations of secrecy –– Member States can adopt specific rules for the powers of the supervisory authorities regarding controllers' and processors' obligation to secrecy.	These provisions are addressing Member States' right to implement more restrictive regulations with regards to processing of certain types of data. They also address special public purposes in the public interest. These provisions are provided for informative purposes only.		
91	Existing data protection rules of churches and religious associations –– Churches and religious associations or communities that lay down their own rules for processing in order to protect natural persons can continue to use those rules as long as they are in line with this Regulation.			
	Delegating acts and implementing acts			
92	Exercise of the delegation –– The Commission has the power to adopt delegated acts. Delegation of power can be revoked at any time by the European Parliament or the Council.	These provisions relate to Commission's power to delegate power. These provisions are provided for informative purposes only.		
93	Committee procedure –– The Commission will be assisted by a committee.			
	Final Provisions			
94	Repeal of directive 95/46/EC –– 1995 Directive 95/46/EC is repealed	Both Druva and its customers, vendors, affiliates, and subcontractors are responsible to ensure compliance with the GDPR by May 25th, 2018		
95	Relationship with Directive 2002/58/EC –– This Regulation does not add obligations for natural or legal persons that are already set out in Directive 2002/58/EC (processing of personal data and the protection of privacy in the electronic communications sector).			
96	Relationship with previously concluded Agreements –– International agreements involving the transfer of data to third countries or organizations that were setup before 24 May 2016 will stay in effect.			
97	Commission reports –– Every four years the Commission will submit a report on this Regulation to the European Parliament and to the Council.			
98	Review of other Union legal acts on data protection –– The Commission can submit legislative proposals to amend other Union legal acts on the protection of personal data.			
99	Entry into force and application –– The Regulation applies from 25 May 2018.			

About Druva

Druva is the global leader in Cloud Data Protection and Management, delivering the industry's first data management-as-a-service solution that aggregates data from endpoints, servers and cloud applications and leverages the public cloud to offer a single pane of glass to enable data protection, governance and intelligence—dramatically increasing the availability and visibility of business critical information, while reducing the risk, cost and complexity of managing and protecting it.

Druva's award-winning solutions intelligently collect data, and unify backup, disaster recovery, archival and governance capabilities onto a single, optimized data set. As the industry's fastest growing data protection provider, Druva is trusted by over 4,000 global organizations, and protects over 100 petabytes of data. Learn more at www.druva.com and join the conversation at twitter.com/druvainc.

druva

Druva, Inc.
Americas: +1 888-248-4976
Europe: +44 (0) 203-7509440
India: +91 (0) 20 6726-3300
Japan: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729
sales@druva.com
www.druva.com